10/502309
PCT/FR 03/00288

R E P U B L I Q U E F R A N Ç A I S E

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 27 JAN. 2003

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

DOCUMENT DE PRIORITÉ

PRÉSENTÉ OU TRANSMIS CONFORMÉMENT À LA RÈGLE 17.1.a) OU b)

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr

INPI
INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11354*01

REQUÊTE EN DÉLIVRANCE 1/2

Cet imprimé est à remplir lisiblement à l'encre noire — DB 540 W / 260899

Réservé à l'INPI

REMISE DES PIÈCES DATE	1 FEV. 2002
LIEU	74
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI	0201435
DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI	01 FEV. 2002

Vos références pour ce dossier *(facultatif)* PB 3988

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

Cabinet PONCET
7 chemin de Tillier
B.P 317
74008 ANNECY CEDEX

Confirmation d'un dépôt par télécopie ☐ N° attribué par l'INPI à la télécopie

2 NATURE DE LA DEMANDE	**Cochez l'une des 4 cases suivantes**
Demande de brevet	☒
Demande de certificat d'utilité	☐
Demande divisionnaire	☐
Demande de brevet initiale	N° Date __/__/____
ou demande de certificat d'utilité initiale	N° Date __/__/____
Transformation d'une demande de brevet européen *Demande de brevet initiale*	☐ N° Date __/__/____

3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)

PROCEDE ET DISPOSITIF POUR SECURISER LES MESSAGES ECHANGES SUR UN RESEAU.

4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE	Pays ou organisation Date __/__/____ N° Pays ou organisation Date __/__/____ N° Pays ou organisation Date __/__/____ N° ☐ **S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»**
5 DEMANDEUR	☐ **S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé «Suite»**
Nom ou dénomination sociale	TRUSTED LOGIC
Prénoms	
Forme juridique	société anonyme
N° SIREN	4 2 1 4 8 3 4 1 3
Code APE-NAF	7 2 1 Z
Adresse — Rue	5 rue du Bailliage
Adresse — Code postal et ville	78000 VERSAILLES
Pays	FRANCE
Nationalité	FRANCAISE
N° de téléphone *(facultatif)*	
N° de télécopie *(facultatif)*	
Adresse électronique *(facultatif)*	

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

REQUÊTE EN DÉLIVRANCE 2/2

Réservé à l'INPI

REMISE DES PIÈCES DATE : 07 JUIL. 2000

LIEU : 74

N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI : 0201435

DB 540 W /260899

Vos références pour ce dossier : *(facultatif)*		PB 3988
6 MANDATAIRE		
Nom		PONCET
Prénom		Jean-François
Cabinet ou Société		Cabinet PONCET
N °de pouvoir permanent et/ou de lien contractuel		
Adresse	Rue	7 chemin de Tillier B.P 317
	Code postal et ville	74008 ANNECY CEDEX
N° de téléphone *(facultatif)*		04 50 51 51 26
N° de télécopie *(facultatif)*		04 50 45 05 82
Adresse électronique *(facultatif)*		PONCET.JF@WANADOO.FR
7 INVENTEUR (S)		
Les inventeurs sont les demandeurs		☐ Oui ☒ Non **Dans ce cas fournir une désignation d'inventeur(s) séparée**
8 RAPPORT DE RECHERCHE		**Uniquement pour une demande de brevet (y compris division et transformation)**
Établissement immédiat ou établissement différé		☒ ☐
Paiement échelonné de la redevance		**Paiement en trois versements, uniquement pour les personnes physiques** ☐ Oui ☐ Non
9 RÉDUCTION DU TAUX DES REDEVANCES		**Uniquement pour les personnes physiques** ☐ Requise pour la première fois pour cette invention *(joindre un avis de non-imposition)* ☐ Requise antérieurement à ce dépôt *(joindre une copie de la décision d'admission pour cette invention ou indiquer sa référence) :*
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes		

10 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (Nom et qualité du signataire)

J-F PONCET, CPI N° 92-1201

VISA DE LA PRÉFECTURE OU DE L'INPI

PROCEDE ET DISPOSITIF POUR SECURISER LES MESSAGES ECHANGES SUR UN RESEAU

La présente invention concerne les systèmes d'information à réseau de transmission de données dans lesquels la communication entre un serveur et un client s'effectue par l'intermédiaire du réseau sous le contrôle d'une autorité qui définit des règles concernant cette communication.

Le contrôle effectif des communications par l'autorité nécessite de contacter directement l'autorité en permanence, ce qui exige une connexion permanente à distance.

Le contrôle effectif de la communication par l'autorité est souvent difficile à mettre en œuvre, en particulier dans des situations où l'autorité ne peut être directement contactée, dans des situations où l'autorité ne souhaite pas être directement impliquée dans une transaction, ou dans des situations où le client et le serveur ne peuvent pas entrer directement en contact.

Le problème proposé par l'invention est de concevoir une nouvelle architecture de système d'information à réseau, dans laquelle un contrôle puisse être exécuté par une autorité sans nécessiter une connexion permanente avec l'autorité.

On cherche simultanément à s'assurer que le contrôle est réalisé en permanence, de sorte que les transmissions soient correctement sécurisées.

L'idée qui est à la base de l'invention est d'assurer le contrôle effectif et permanent de la communication par un représentant de l'autorité qui est implémenté dans ou à proximité immédiate du client, de sorte que l'invention peut s'appliquer à des architectures dans lesquelles le client est de petite taille et ne comporte pas en lui-même les ressources nécessaires pour remplir les fonctions de sécurité et les autres fonctions de représentant de l'autorité.

Pour atteindre ces buts ainsi que d'autres, l'invention prévoit un procédé pour sécuriser les messages échangés sur un réseau de transmission de données entre un serveur et un client, sous le contrôle d'une autorité qui définit les règles d'échange des messages ; selon l'invention le contrôle est assuré de manière décentralisée par un représentant de l'autorité, intercalé en

permanence dans le réseau entre le serveur et le client, à proximité du client, pendant l'échange sécurisé des messages, effectuant une traduction des messages transmis et effectuant sur les messages transmis les contrôles décidés par l'autorité.

Selon un mode de réalisation avantageux, on utilise un premier protocole pour les échanges entre le serveur et le représentant de l'autorité, et on utilise un second protocole différent du premier protocole pour les échanges entre le représentant de l'autorité et le client.

En pratique, pour l'échange de messages selon l'invention :

- on établit entre le serveur et le représentant de l'autorité un premier canal sécurisé en utilisant une première clé connue du représentant de l'autorité et du serveur mais pas du client, et en utilisant un premier algorithme de cryptage,
- on établit entre le représentant de l'autorité et le client un second canal sécurisé en utilisant une seconde clé connue du représentant de l'autorité et du client mais pas du serveur, et en utilisant un second algorithme de cryptage.

L'invention prévoit également un dispositif pour sécuriser les messages échangés sur un réseau de transmission de données entre un serveur et un client sous le contrôle d'une autorité qui définit les règles d'échange des messages ; selon l'invention on prévoit un dispositif de contrôle décentralisé ou représentant de l'autorité, intercalé en permanence dans le réseau entre le serveur et le client, à proximité du client, pendant l'échange sécurisé des messages, effectuant une traduction des messages transmis, et effectuant sur les messages transmis les contrôles décidés par l'autorité.

Selon un mode de réalisation avantageux, le dispositif de contrôle décentralisé ou représentant de l'autorité est un microsystème informatique matériellement sécurisé, intercalé en permanence entre le serveur et le client pendant l'échange sécurisé des messages.

On peut avantageusement prévoir que :

- le serveur est un système informatique comprenant un port d'entrée-sortie ;

- le client est un microsystème informatique comprenant un port d'entrée-sortie ;
- le représentant de l'autorité est un microsystème informatique matériellement sécurisé comprenant un dispositif d'interface ;
- un système spécifique d'interfaçage est prévu, comprenant un port d'entrée-sortie connecté au port d'entrée-sortie du système informatique serveur, comprenant un port de cartes connecté au port d'entrée-sortie du microsystème informatique client, comprenant un port d'entrée-sortie connecté au dispositif d'interface du microsystème informatique représentant l'autorité, et comprenant un contrôleur programmé pour contrôler les communications entre les ports d'entrée-sortie ;
- le contrôleur et le représentant de l'autorité sont programmés de façon que :
  - le système informatique serveur envoie une requête A au microsystème informatique client, et cette requête est reçue par le contrôleur ;
  - le contrôleur transmet la requête A au représentant de l'autorité, qui lui retourne une réponse Ra ;
  - cette réponse Ra est utilisée par le contrôleur pour calculer une requête A' qui est envoyée au microsystème informatique client ;
  - la requête A' est traitée par le microsystème informatique client, qui prépare une réponse B' ;
  - le microsystème informatique client envoie la réponse B' au système informatique serveur ; cette réponse est reçue par le contrôleur ;
  - le contrôleur transmet la réponse B' au représentant de l'autorité, qui lui retourne une réponse Rb ;
  - cette réponse Rb est utilisée par le contrôleur pour calculer une réponse B qui est envoyée au système informatique serveur.

Selon une première application, on peut prévoir que :
- le client est une carte à microprocesseur ;
- le représentant de l'autorité est une carte à microprocesseur ;
- le système spécifique d'interfaçage est un lecteur de cartes à microprocesseur comportant deux ports de cartes.

Selon une seconde application, on peut prévoir que :

- le client est un système mobile de communication ;
- le serveur est un système informatique communiquant avec le client par une connexion physique ou par un réseau de communication sans fil ;
- le représentant de l'autorité est une carte à microprocesseur représentant l'opérateur du réseau de communication sans fil (dite carte SIM dans les téléphones répondant aux normes GSM).

Selon une troisième application, on peut prévoir que :

- le client est une carte à microprocesseur ;
- le représentant de l'autorité est un système informatique matériellement sécurisé ;
- le système spécifique d'interfaçage est une machine comportant un port de cartes et une interface d'entrée-sortie spécifique de liaison avec le système informatique représentant de l'autorité.

D'autres objets, caractéristiques et avantages de la présente invention ressortiront de la description suivante de modes de réalisation particuliers, faite en relation avec les figures jointes, parmi lesquelles:

- la figure 1 illustre schématiquement l'échange des messages entre le serveur et le client selon la solution générale de la présente invention ;
- la figure 2 illustre l'échange des messages entre serveur et client, dans l'application au téléchargement d'un code exécutable ;
- la figure 3 illustre la transmission de messages du serveur vers le client dans une application de cryptographie à clé publique ;
- la figure 4 illustre un mode de réalisation de l'invention où le serveur est un système informatique, et le client est une carte à microprocesseur, connectée au système informatique par le biais d'un lecteur de cartes à microprocesseur ;
- la figure 5 illustre un mode de réalisation selon la figure 4, et où le représentant de l'autorité est implémenté dans une autre carte à microprocesseur connectée au même lecteur de cartes ;
- la figure 6 illustre le flux de la requête envoyée du serveur au client dans le mode de réalisation de la figure 5 ; et
- la figure 7 illustre le flux de la réponse envoyée du client au serveur dans le mode de réalisation de la figure 5.

Comme illustré de façon générale sur la figure 1, un dispositif pour sécuriser les messages échangés sur un réseau de transmission de données entre un serveur 1 et un client 2, sous le contrôle d'une autorité qui définit les règles d'échange des messages, comprend un dispositif de contrôle décentralisé, constitué par un représentant de l'autorité 3, intercalé en permanence dans le réseau entre le serveur 1 et le client 2 pendant l'échange sécurisé de messages.

Le représentant de l'autorité 3 effectue une traduction des messages, ainsi que des actions décidées par l'autorité.

Du point de vue des protocoles, ce représentant de l'autorité 3 est entièrement transparent, dans la mesure où le serveur 1 communique avec lui comme avec un de ses clients, et le client 2 communique avec lui comme avec un serveur.

Par contre, il est dès lors possible d'avoir des protocoles différents, soit un premier protocole P entre le serveur 1 et le représentant de l'autorité 3, et un second protocole P' entre le représentant de l'autorité 3 et le client 2. Le message A transmis par le serveur 1 est transformé par le représentant de l'autorité 3 en un message A' reçu par le client 2. En retour, le message de réponse B' émis par le client 2 est transformé par le représentant de l'autorité 3 en un message B reçu par le serveur 1.

Le représentant de l'autorité 3, réalisant un dispositif de contrôle décentralisé, peut avantageusement être disposé à proximité du client 2.

Une solution avantageuse consiste à implémenter le représentant de l'autorité 3 dans une carte à microprocesseur spécifique, intercalée en permanence entre le serveur 1 et le client 2 pendant l'échange sécurisé de messages.

Le représentant de l'autorité 3 détient des secrets appartenant à l'autorité, qui permettent d'assurer qu'une communication entre le serveur 1 et le client 2 ne peut être établie que sous son contrôle. Un protocole cryptographique peut avantageusement être utilisé pour s'assurer de l'utilisation du représentant de l'autorité 3.

Dans le cas où le représentant de l'autorité 3 est implémenté dans une carte à microprocesseur, cela permet de

s'assurer que les secrets détenus par ce représentant de l'autorité 3 sont abrités d'attaques extérieures.

On décrira maintenant un premier exemple d'utilisation de l'invention, pour la vérification d'un code exécutable devant être téléchargé dans le client 2. Cette application est décrite en relation avec la figure 2.

Un serveur 1 peut être amené dans certains cas à télécharger du code exécutable dans un client 2. Toutefois, ce code doit répondre à un ensemble de propriétés qui doivent être vérifiées par une autorité de vérification avant d'autoriser ce chargement. Ces vérifications sont destinées à assurer la sécurité du client, et sont donc généralement sous la responsabilité du propriétaire du client.

L'invention s'adresse au cas où le client 2 est un microsystème informatique tel qu'une carte à microprocesseur ou un autre système embarqué aux capacités sécuritaires limitées, par exemple un téléphone cellulaire ou un assistant numérique personnel. Le chargement de programmes doit s'effectuer par le biais d'un canal sécurisé entre le serveur et le client, canal sécurisé qui permet de garantir l'intégrité et/ou la confidentialité des informations transmises sur le canal. L'établissement de ce canal nécessite l'existence d'un secret cryptographique partagé (clé K) entre le client 2 et le serveur 1.

Selon l'invention, on peut utiliser une carte à microprocesseur spécifique, qui représente l'autorité de vérification et constitue le représentant de l'autorité 3. La carte à microprocesseur est intercalée entre le serveur 1 et le client 2. Ce représentant de l'autorité 3 peut alors effectuer toutes les vérifications nécessaires. Il établit deux canaux sécurisés pour l'échange des messages :

- entre le serveur 1 et le représentant de l'autorité 3, un premier canal sécurisé 4 en utilisant une première clé Ks connue du représentant de l'autorité 3 et du serveur 1 mais pas du client 2, et en utilisant un premier algorithme de cryptage AL,
- entre le représentant de l'autorité 3 et le client 2 un second canal sécurisé 5 en utilisant une seconde clé Kc connue du

représentant de l'autorité 3 et du client 2 mais pas du serveur 1, et en utilisant un second algorithme de cryptage AL'.

Cela permet d'assurer que la communication entre le client 2 et le serveur 1 ne peut être établie qu'à travers le représentant de l'autorité 3, et donc que les vérifications nécessaires sont effectuées.

Un chargement de code peut alors s'effectuer de la manière suivante :

- le serveur 1 établit un premier canal sécurisé 4 avec le représentant de l'autorité 3, en utilisant la clé Ks et l'algorithme AL ;
- le serveur 1 envoie le code à charger C au représentant de l'autorité 3, par le biais du premier canal sécurisé 4 ; on note sur la figure 2 l'indication C(AL)Ks pour indiquer que le code C est sécurisé par l'algorithme AL et la clé Ks (signature et/ou chiffrement) ;
- le représentant de l'autorité 3 vérifie les propriétés sur le code C ; on dénote par VC le code ainsi vérifié, auquel il peut être ajouté une preuve que la vérification a bien été effectuée ;
- le représentant de l'autorité 3 établit un second canal sécurisé 5 avec le client 2, en utilisant la clé Kc et l'algorithme AL' ;
- le représentant de l'autorité 3 envoie le code vérifié VC au client 2 en utilisant le second canal sécurisé 5 établi ci-dessus ; il transmet donc VC(AL')Kc ;
- si nécessaire, le client 2 renvoie une preuve de chargement P par le biais du second canal sécurisé 5 : il envoie donc P(AL')Kc ; le représentant de l'autorité 3 traduit alors ce message en utilisant P(AL)Ks pour communiquer avec le serveur 1.

Cette solution comporte de nombreux avantages : la vérification peut être effectuée de manière systématique, sans toutefois nécessiter une communication directe avec l'autorité de vérification ; et la vérification peut être effectuée sans nécessiter aucun changement du client ou du serveur : pour le serveur 1, le représentant de l'autorité 3 se comporte comme un client ; pour le client 2, le représentant de l'autorité 3 se comporte comme un serveur.

En outre, la solution selon l'invention ne nécessite pas de ressource supplémentaire dans le client 2 pour effectuer la vérification. Elle ne nécessite pas, non plus, que le client 2 soit en mesure de vérifier des signatures électroniques. Egalement, la solution assure une grande flexibilité. Enfin, la solution permet une implantation dans une carte à microprocesseur, qui peut ainsi fonctionner dans des environnements non connectés.

On décrira maintenant un second exemple d'application de l'invention à la cryptographie à clé publique.

Certains protocoles cryptographiques utilisés avec des cartes à microprocesseur sont basés sur l'utilisation de cryptographie à clés publiques. Toutefois, ces techniques cryptographiques sont coûteuses, et ne sont donc pas supportées par toutes les cartes à microprocesseur.

Un cas particulièrement intéressant réside dans la vérification de signatures électroniques permettant par exemple de garantir l'origine d'une donnée téléchargée. Ces signatures électroniques sont généralement implémentées à l'aide d'algorithmes à clé publique. Mais cela pose un problème aux cartes à microprocesseur les plus simples, et à d'autres systèmes simples, à cause des ressources importantes nécessaires pour utiliser l'algorithme. Ces algorithmes reposent sur une paire de clés (Kpriv, Kpub). La clé Kpriv est utilisée par le serveur 1 pour calculer la signature de la données, et ne doit être connue que du seul serveur 1. La clé Kpub est utilisée pour vérifier la signature de la donnée par le client 2, et elle peut être diffusée sans contrainte de confidentialité.

Selon l'invention on intercale, entre le serveur 1 qui envoie la donnée à signature électronique et le client 2 qui reçoit la donnée et vérifie la signature électronique, un représentant de l'autorité 3 de contrôle du client 2. Ce représentant de l'autorité 3 sera chargé de vérifier la signature électronique au nom du client 2 et ensuite de lui communiquer la donnée par le biais d'un canal sécurisé par une clé Kc, connue uniquement du représentant de l'autorité 3 et du client 2.

Le processus de communication est illustré sur la figure 3 :

- le serveur 1 calcule la signature de la donnée D avec la clé Kpriv et l'algorithme AL. Le résultat est D(AL)Kpriv ;
- le serveur 1 communique la donnée D et la signature au représentant de l'autorité 3, éventuellement par le biais d'un premier canal sécurisé 4 ;
- le représentant de l'autorité 3 vérifie la signature et la donnée D ;
- le représentant de l'autorité 3 établit un second canal sécurisé 5 avec le client 2 au moyen de la clé Kc et de l'algorithme AL' ;
- le représentant de l'autorité 3 transmet la donnée D sous la forme D(AL')Kc, sans la signature, au client 2 par le biais du second canal sécurisé 5.

Contrairement au premier exemple précédent, le représentant de l'autorité 3 n'est pas entièrement transparent, dans la mesure où le protocole utilisé entre le serveur 1 et le représentant de l'autorité 3 diffère du protocole utilisé entre le représentant de l'autorité 3 et le client 2. Cette solution peut d'ailleurs être utilisée dans d'autres cas où des traductions de protocole sont nécessaires.

Dans les exemples ci-dessus, l'utilisation d'un représentant de l'autorité 3 est rendue transparente pour le serveur 1 et pour le client 2 d'un point de vue logique, mais les messages doivent toutefois être acheminés physiquement vers le représentant de l'autorité 3 au lieu d'être acheminés vers le client 2. Il est donc nécessaire que le serveur 1 soit programmé pour communiquer avec le représentant de l'autorité 3, et non pas pour communiquer avec le client 2.

Dans les cas où le serveur 1 est classiquement programmé pour communiquer directement avec le client 2, et où le serveur 1 est un système informatique et le client 2 est une carte à microprocesseur, l'invention propose par exemple d'intégrer le mécanisme de représentant de l'autorité 3, soit de façon permanente dans un lecteur de cartes à microprocesseur 7 connectant le système informatique serveur 1 à la carte cliente 2, comme illustré sur la figure 4, soit de façon amovible dans une carte à microprocesseur distincte connectée au lecteur de carte à microprocesseur 7, comme illustré sur la figure 5. Dans ce mode de réalisation de la figure

5, le système informatique serveur 1 comprend un port d'entrée-sortie 1a. Le système informatique serveur 1 est associé au lecteur de cartes à microprocesseur 7 qui comprend un port d'entrée-sortie 8 connecté au port d'entrée-sortie 1a du système informatique serveur 1. Le lecteur de cartes à microprocesseur 7 comprend un port de cartes 10 adapté pour connecter une carte à microprocesseur 3 représentant l'autorité, et un port de cartes 9 adapté pour connecter une carte à microprocesseur 2, le client dans cette réalisation. La carte à microprocesseur 2 comprend un port d'entrée-sortie 12 connecté au port de cartes 9. Le lecteur de cartes à microprocesseur 7 comprend également un contrôleur 11 programmé pour contrôler les communications entre le port d'entrée-sortie 8, le port de cartes 10, et le port de cartes 9.

La carte à microprocesseur 3 connectée au port de cartes 10 définit ainsi un représentant de l'autorité.

Le contrôleur 11, et la carte à microprocesseur 3 (le représentant de l'autorité) sont programmés de façon que les flux de données se déroulent comme illustré sur la figure 6 pour une requête envoyée du système informatique serveur 1 vers la carte à microprocesseur cliente 2, et comme illustré sur la figure 7 pour une réponse retournée de la carte à microprocesseur cliente 2 vers le système informatique serveur 1.

Pour le flux de la requête envoyée du système informatique serveur 1 vers la carte à microprocesseur cliente 2 (figure 6):

- le système informatique serveur 1 envoie une requête A à la carte à microprocesseur cliente 2. Cette requête est reçue par le contrôleur 11 ;
- le contrôleur 11 transmet la requête A au représentant de l'autorité 3, qui lui retourne une réponse Ra ;
- cette réponse Ra est utilisée par le contrôleur 11 pour calculer une requête A' qui est envoyée à la carte à microprocesseur cliente 2.

Le flux de réponse retourné par la carte à microprocesseur cliente 2 au système informatique serveur 1 se déroule de la façon suivante (figure 7):

- la carte à microprocesseur cliente 2 envoie une réponse B' au système informatique serveur 1. Cette réponse est reçue par le contrôleur 11 ;
- le contrôleur 11 transmet la réponse B' au représentant de l'autorité 3, qui lui retourne une réponse Rb ;
- cette réponse Rb est utilisée par le contrôleur 11 pour calculer une réponse B qui est envoyée au système informatique serveur 1.

Dans le cas le plus simple, les réponses Ra et Rb peuvent être une simple encapsulation des messages transformés A et B'.

Les figures 5 à 7 peuvent aussi servir pour illustrer le mode de réalisation dans lequel le représentant de l'autorité 3 est un microsystème informatique matériellement sécurisé, comprenant un dispositif d'interface 13. Le port d'entrée-sortie 10 du système d'interfaçage 7 est alors raccordé au dispositif d'interface 13.

La présente invention n'est pas limitée aux modes de réalisation qui ont été explicitement décrits, mais elle en inclut les diverses variantes et généralisations contenues dans le domaine des revendications ci-après.

REVENDICATIONS

1 - Procédé pour sécuriser les messages échangés sur un réseau de transmission de données entre un serveur (1) et un client (2) de petite taille et ne comportant pas en lui-même les ressources nécessaires pour remplir les fonctions de sécurité, sous le contrôle d'une autorité qui définit les règles d'échange des messages, caractérisé en ce que le contrôle est assuré de manière décentralisée par un représentant de l'autorité (3), intercalé en permanence dans le réseau à proximité du client (2) et entre le serveur (1) et le client (2) pendant l'échange sécurisé des messages, effectuant une traduction des messages transmis et effectuant sur les messages transmis les contrôles décidés par l'autorité.

2 - Procédé selon la revendication 1, caractérisé en ce qu'on utilise un premier protocole (P) pour les échanges entre le serveur (1) et le représentant de l'autorité (3), et on utilise un second protocole (P') différent du premier protocole (P) pour les échanges entre le représentant de l'autorité (3) et le client (2).

3 - Procédé selon l'une des revendications 1 ou 2, caractérisé en ce que, pour l'échange de messages :
- on établit entre le serveur (1) et le représentant de l'autorité (3) un premier canal sécurisé (4) en utilisant une première clé (Ks) connue du représentant de l'autorité (3) et du serveur (1) mais pas du client (2), et en utilisant un premier algorithme de cryptage (AL),
- on établit entre le représentant de l'autorité (3) et le client (2) un second canal sécurisé (5) en utilisant une seconde clé (Kc) connue du représentant de l'autorité (3) et du client (2) mais pas du serveur (1), et en utilisant un second algorithme de cryptage (AL').

4 - Dispositif pour sécuriser les messages échangés sur un réseau de transmission de données entre un serveur (1) et un client (2) de petite taille et ne comportant pas en lui-même les ressources nécessaires pour remplir la fonction de sécurité, sous le contrôle d'une autorité qui définit les règles d'échange des messages, caractérisé en ce qu'il comprend un dispositif de contrôle décentralisé ou représentant de l'autorité (3), intercalé

en permanence dans le réseau à proximité du client (2) et entre le serveur (1) et le client (2) pendant l'échange sécurisé des messages, effectuant une traduction des messages transmis, et effectuant sur les messages transmis les contrôles décidés par l'autorité.

5 - Dispositif selon la revendication 4, caractérisé en ce que le dispositif de contrôle décentralisé ou représentant de l'autorité (3) est un microsystème informatique matériellement sécurisé, intercalé en permanence entre le serveur (1) et le client (2) pendant l'échange des messages.

6- Dispositif selon la revendication 5, caractérisé en ce que :

- le serveur (1) est un système informatique comprenant un port d'entrée-sortie (1a) ;
- le client (2) est un microsystème informatique comprenant un port d'entrée-sortie (12) ;
- le représentant de l'autorité (3) est un microsystème informatique matériellement sécurisé comprenant un dispositif d'interface (13) ;
- un système spécifique d'interfaçage (7) est prévu, comprenant un port d'entrée-sortie (8) connecté au port d'entrée-sortie (1a) du système informatique serveur (1), comprenant un port de cartes (9) connecté au port d'entrée-sortie (12) du microsystème informatique client (2), comprenant un port d'entrée-sortie (10) connecté au dispositif d'interface (13) du microsystème informatique représentant l'autorité (3), et comprenant un contrôleur (11) programmé pour contrôler les communications entre les ports d'entrée-sortie (8), (9) et (10) ;
- le contrôleur (11) et le représentant de l'autorité (3) sont programmés de façon que :
  - le système informatique serveur (1) envoie une requête A au microsystème informatique client (2), et cette requête est reçue par le contrôleur (11) ;
  - le contrôleur (11) transmet la requête A au représentant de l'autorité (3), qui lui retourne une réponse Ra ;

- cette réponse Ra est utilisée par le contrôleur (11) pour calculer une requête A' qui est envoyée au microsystème informatique client (2) ;
- la requête A' est traitée par le microsystème informatique client (2), qui prépare une réponse B' ;
- le microsystème informatique client (2) envoie la réponse B' au système informatique serveur (1) ; cette réponse est reçue par le contrôleur (11) ;
- le contrôleur (11) transmet la réponse B' au représentant de l'autorité (3), qui lui retourne une réponse Rb ;
- cette réponse Rb est utilisée par le contrôleur (11) pour calculer une réponse B qui est envoyée au système informatique serveur (1).

7 - Dispositif selon la revendication 6, caractérisé en ce que :
- le client (2) est une carte à microprocesseur ;
- le représentant de l'autorité (3) est une carte à microprocesseur ;
- le système spécifique d'interfaçage est un lecteur de cartes à microprocesseur (7) comportant deux ports de cartes (9) et (10).

8 - Dispositif selon la revendication 6, caractérisé en ce que :
- le client (2) est un système mobile de communication ;
- le serveur (1) est un système informatique communiquant avec le client (2) par une connexion physique ou par un réseau de communication sans fil ;
- le représentant de l'autorité (3) est une carte à microprocesseur représentant l'opérateur du réseau de communication sans fil (dite carte SIM dans les téléphones répondant aux normes GSM).

9 - Dispositif selon la revendication 6, caractérisé en ce que :
- le client (2) est une carte à microprocesseur ;
- le représentant de l'autorité (3) est un système informatique matériellement sécurisé ;
- le système spécifique d'interfaçage (7) est une machine comportant un port de cartes (9) et une interface d'entrée-sortie

spécifique (10) de liaison avec le système informatique représentant de l'autorité (3).

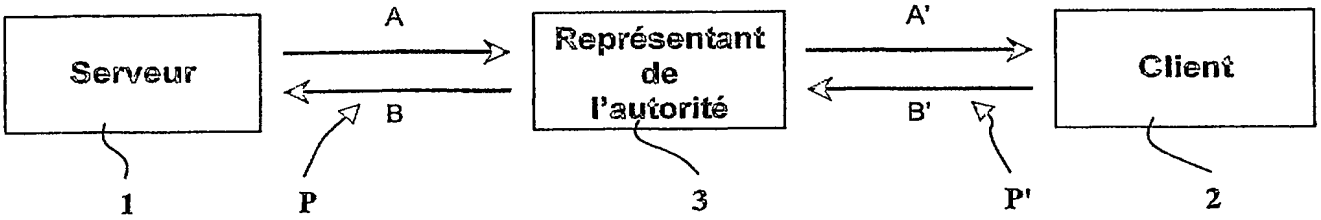

FIG. 1

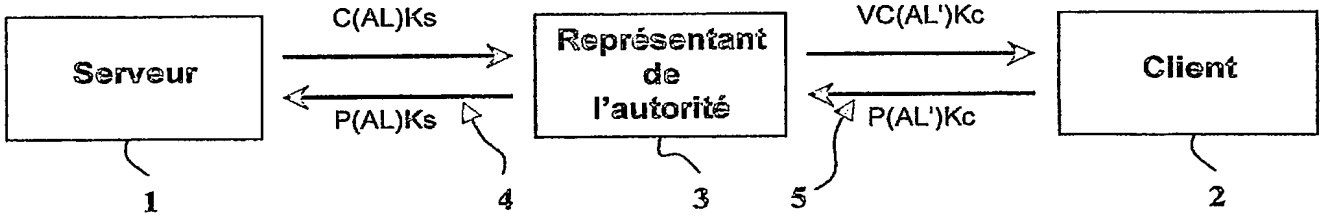

FIG. 2

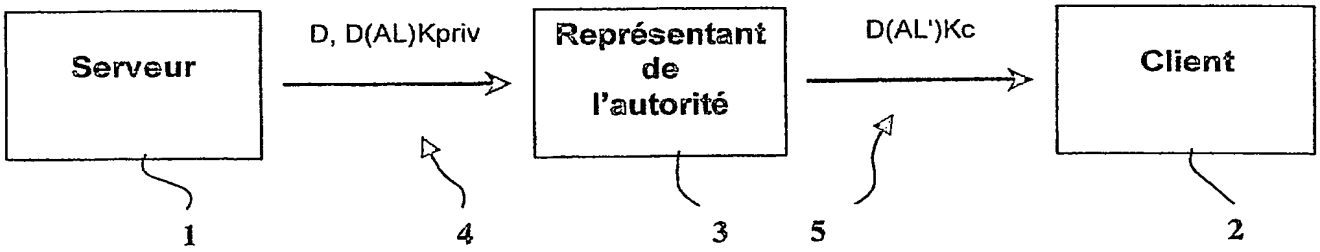

FIG. 3

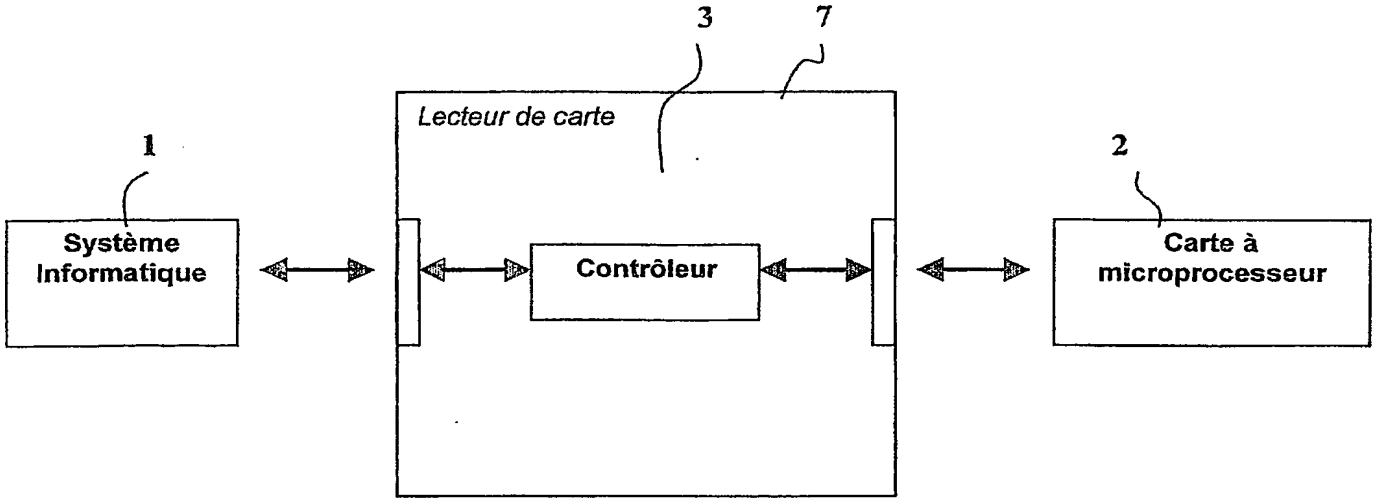
3
7
Lecteur de carte
1
2
Système Informatique
Contrôleur
Carte à microprocesseur

FIG. 4

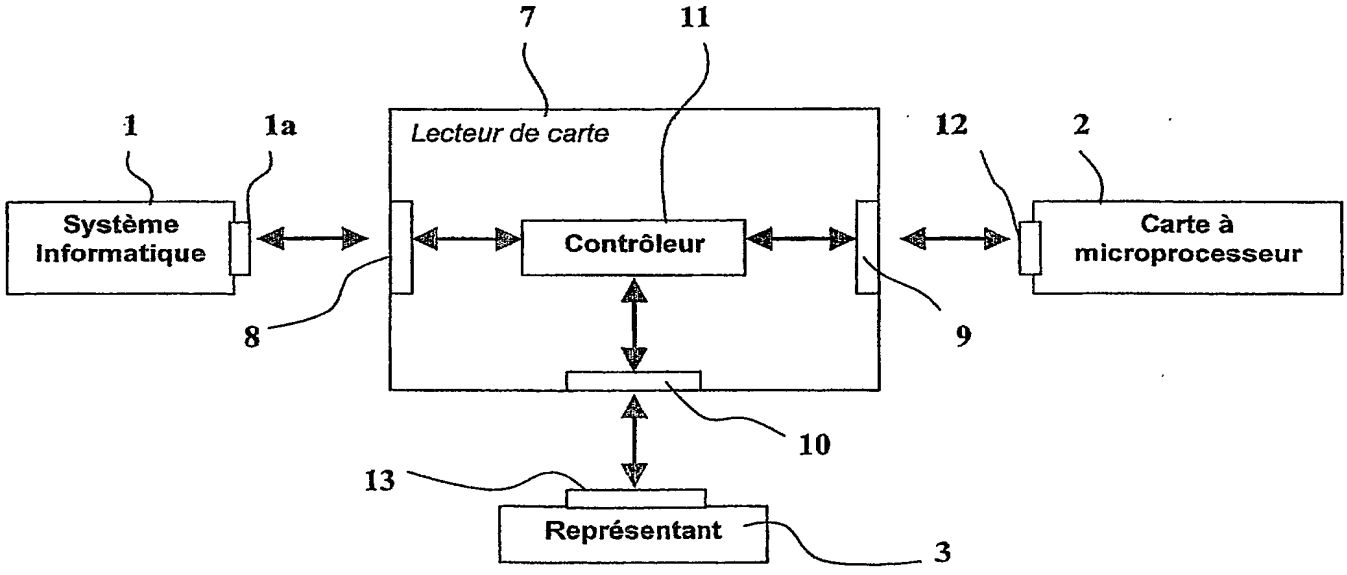
7
11
1
1a
Lecteur de carte
12
2
Système Informatique
Contrôleur
Carte à microprocesseur
8
9
10
13
Représentant
3

FIG. 5

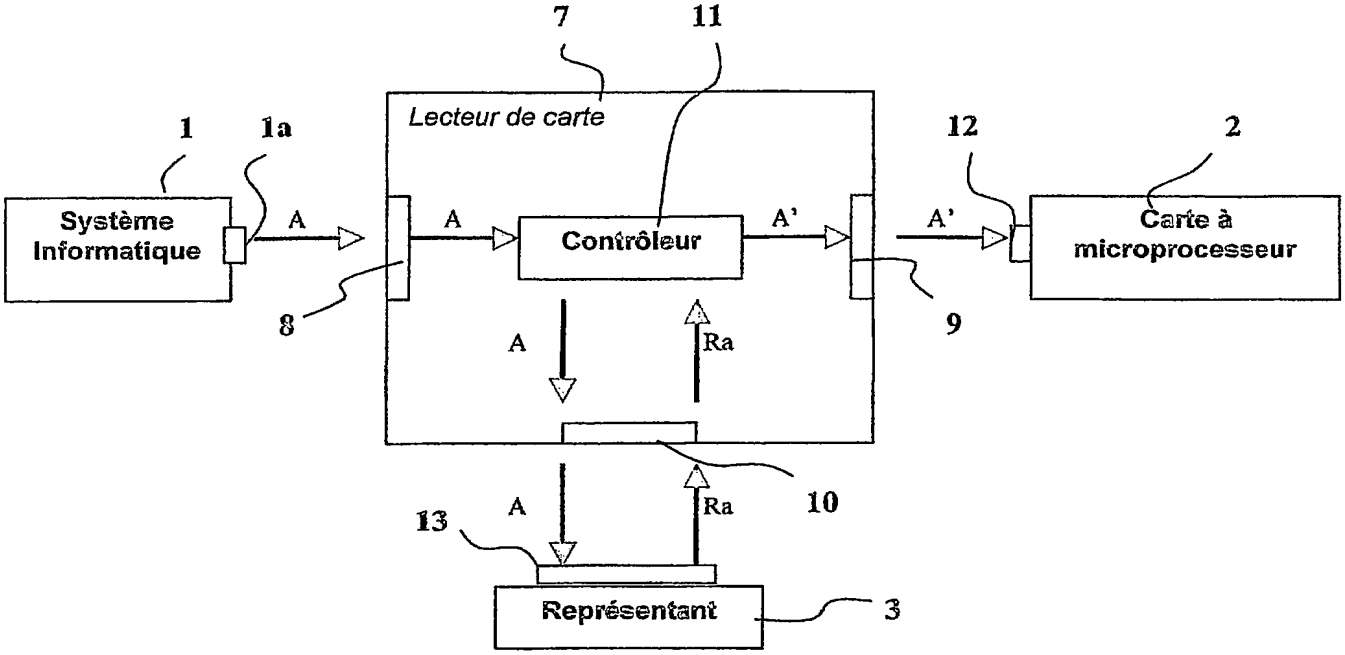
7
11
Lecteur de carte
1
1a
12
2
Système Informatique
A
A
Contrôleur
A'
A'
Carte à microprocesseur
8
9
A
Ra
10
13
A
Ra
Représentant
3

FIG. 6

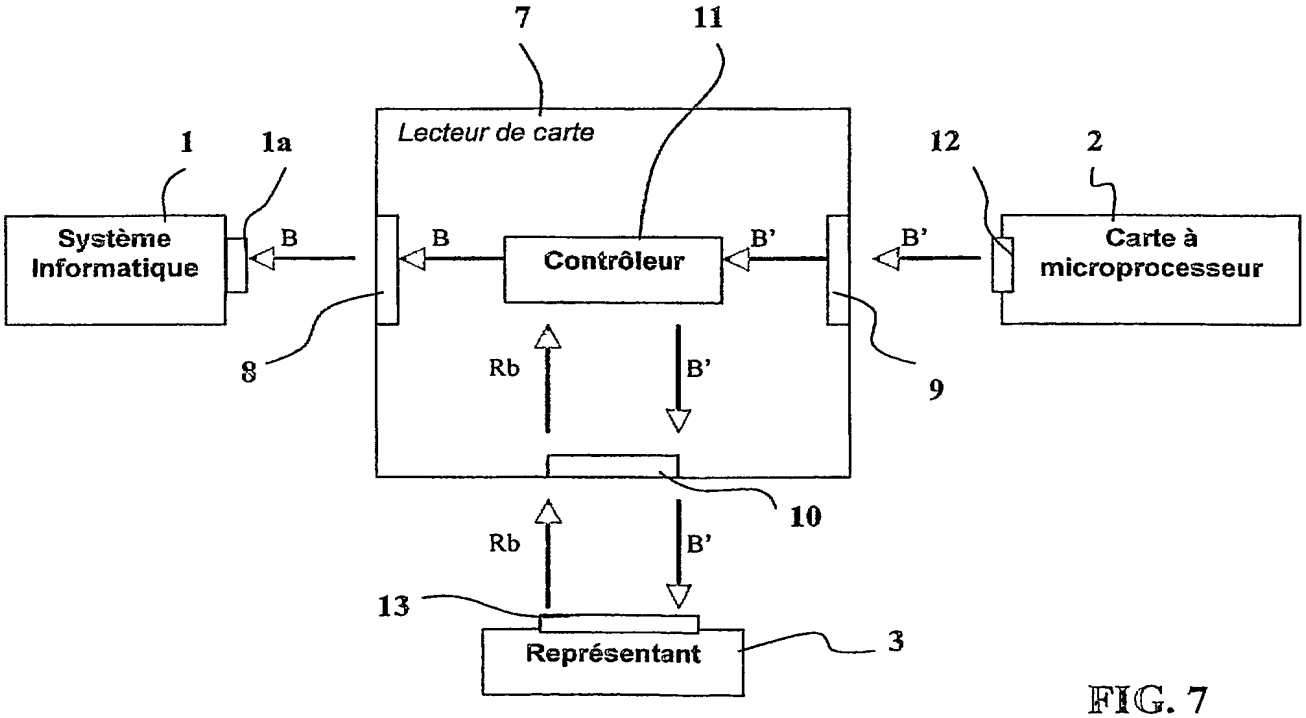
7
11
Lecteur de carte
1
1a
12
2
Système Informatique
B
B
Contrôleur
B'
B'
Carte à microprocesseur
8
9
Rb
B'
10
Rb
B'
13
Représentant
3

FIG. 7

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11 235*02

DÉSIGNATION D'INVENTEUR(S) Page N° 1../1..

(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)

Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 W /260899

Vos références pour ce dossier *(facultatif)*	PB 3988
N° D'ENREGISTREMENT NATIONAL	02 01437

TITRE DE L'INVENTION (200 caractères ou espaces maximum)

PROCEDE ET DISPOSITIF POUR SECURISER LES MESSAGES ECHANGES SUR UN RESEAU.

LE(S) DEMANDEUR(S) :

TRUSTED LOGIC

DESIGNE(NT) EN TANT QU'INVENTEUR(S) : (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).

Nom		VETILLARD	
Prénoms		Eric	
Adresse	Rue	1 Passage des Pignes Bât. 121	
	Code postal et ville	06560	VALBONNE
Société d'appartenance *(facultatif)*			
Nom			
Prénoms			
Adresse	Rue		
	Code postal et ville		
Société d'appartenance *(facultatif)*			
Nom			
Prénoms			
Adresse	Rue		
	Code postal et ville		
Société d'appartenance *(facultatif)*			

DATE ET SIGNATURE(S)
DU (DES) DEMANDEUR(S)
OU DU MANDATAIRE
(Nom et qualité du signataire)

Annecy, le 1er février 2002

J-F PONCET, CPI N° 92-1201

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.